context and the transaction can proceed. It is noted that authentication of the user is considered a special case of authentication of the context. The context may include additional security limitations such as location etc which are additional to verifying the real identity of the user.

[0063] The system also includes a plurality of authentication mechanisms **10**, **11** and **12** each exhibiting a confidence which can be placed in the result of using the corresponding mechanism. These means are functional elements which are used to dynamically provide the confidence engine with confidence parameters relating to the security or other aspects of the transaction context.

[0064] Examples of authentication mechanisms include the type of user device into which the transaction request **14** is input. In the case of a PDA, its data may be protected by a robust password system and the device itself always be in the possession of the user. Therefore, as an authentication mechanism, the system would have a high degree of confidence in its use.

[0065] In some situations, the device capability can be the defining characteristic of the transaction context. Therefore it can be considered as a separate functional block **13**.

[0066] Another example of an authentication mechanism (**10**, **11**, **12**) is a location system. Here the transaction may require a user to be in a specified location for authentication to be achieved. For example, a user of a corporate intranet may only be allowed access to certain resource when he or she is physically on the business site. In this case the system checks that the user is at the required location and authentication is not achieved if the user is not at the required location.

[0067] Another example of an authentication mechanism is multiple-user of multiple-individual collocation. Here, the transaction may require the physical presence of two specified individuals at the same location, each carrying out a binary login authentication. Such a context might be found where unaccompanied access to extremely sensitive information is forbidden or illegal. Sensing and/or location hardware in conjunction with each individuals binary login device could be used to verify the collocation. For a highly sensitive database or a financial transaction, the system might require a collocation, i.e.: the presence of two identified people and/or viewing the resource from at a specified location. In this case, an appropriate authentication mechanism such as proximity sensing hardware or the Global Positioning System could be used to authenticate the users.

[0068] The system illustrated in **FIG. 1** may also implement a Guard and Monitor functional unit **16**. This can be configured as a proxy server to handle and monitor access to the Resources **17**. The proxy is configured to act as a firewall and screen access to the resources depending on whether the transaction has been authenticated.

[0069] A configuration engine **18** may be included. This is a functional unit which handles and coordinates interactions between other funcational components of the system. It manages profile information and other housekeeping information related to the rules applied TO contexts as well as potentially checking the transaction status and requirements.

[0070] In many transaction contexts there are certain confidence parameters which can be considered as fundamental and substantially unchanging. In such cases it can be useful to define a static confidence window. This construct is an expected confidence range which is defined in response to substantially static confidence parameters,

[0071] The confidence window has an upper and lower limit reflecting an inherent upper and lower limit that the confidence level can potentially reach given the lack of variability in the static confidence parameters. An example of a static fundamental confidence parameter corresponds to the location of a user. Another example might be the situation where the machine storing the requested resources has some longstanding security limitation such as vulnerability to certain viruses or hacking attempts. These security limitations will set an inherent fixed upper limit beyond which the confidence level cannot extend. If the machine on which the requested resources resides is fundamentally limited in its security, there may be contexts where no external authentication act can improve the confidence level to a point where authentication can be achieved.

[0072] This embodiment of the invention can be used to simplify the process of comparing the dynamically determined confidence level with the confidence threshold. That is, it can be viewed as a coarse filter which tests the context level for potential future fundamental lack of security compliance given the inherent limitations in the confidence of the system.

[0073] To summarise these definitions:

[0074] The confidence level: corresponds to the current dynamic level of confidence in authentication.

[0075] The confidence window: corresponds to a set of upper and lower bounds to the confidence level that are set by static confidence parameters or elements other than individual confidence events.

[0076] The confidence threshold: corresponds to the level of confidence in the user authentication that is required before a resource may be accessed.

[0077] **FIG. 2** illustrates this situation along with the time progression of a two-step incremental dynamic process for authenticating a users ability to perform a transaction The vertical axis represents the confidence. The variable line represents the confidence level which is determined by dynamically collecting and assessing the plurality of confidence parameters.

[0078] Initially at step **1**, a fast authentication is performed. This may be a binary login which validates the user at a relatively low confidence level. Then, after some time has elapsed, a full authentication **2** is performed taking the confidence level to a high level. Given the specific context confidence assumptions (lack of user input etc), the system allows the confidence to decay **3** until the user performs or is required to perform, a full authentication **4** to re-establish the context confidence level.

[0079] The dynamic confidence level is monitored and compared with a predetermined threshold. If the confidence level drops below a predetermined confidence threshold, the transaction is not authenticated and if the confidence level exceeds a predetermined confidence threshold, the transaction is authenticated.